IN THE SPECIFICATION

Please amend the paragraph on page 3, lines 1-7, as follows:

-- The prior art does not provide a solution to the EAP/SIM authentication problems; in Patel's report a solution by storing all previous used RANDs is discussed but deemed impractical. (In UMTS (Universal Mobile Telecommunications System) security, the replay problem of GSM has been taken into account and removed by a specification of a complex replay prevention method, which involves both HLR (Home Location Register) and the terminal.) --

Please amend the paragraph from page 6, line 20 to page 7, line 8, as follows:

-- Referring now to Fig. 1, when a (telecommunication) terminal 10 is adapted according to the invention, it uses a special module--including data and a corresponding procedure that can be queried about the data--to store information on used RANDS. If the terminal is dual-mode (i.e. if it is adapted for use with GSM and also UMTS), then it can advantageously use two different special modules: a so-called MWLAN module 11 (i.e. module for the WLAN mode) in which the terminal stores information on RANDs that have been used for EAP SIM authentication; and a MGSM module 12 (i.e. module for the GSM mode) in which the terminal stores information on RANDs used for GSM. When the terminal 10 receives a new challenge RAND for EAP SIM authentication, it passes it to an authenticator module 14, which checks it against the information stored in the MWLAN module 11 and also the MGSM module 12 to determine whether the RAND has been used before, by querying each of the modules. When the terminal 10 receives a challenge RAND for GSM authentication, it passes the challenge RAND to the authenticator module 14, which then verifies that the RAND has not previously been used for EAP SIM authentication using information stored in the MWLAN data store 11. After checking the appropriate module(s) 11 12, the terminal 10 provides a RAND challenge response. --